

Индивидуальный проект – этап 4

Кузьмин Артем

16 марта, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Целью данной работы является изучение сканера уязвимостей nikto.

Выполнение лабораторной работы

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности.

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе. Сканирование веб-сервера

```
perl nikto.pl -h
```

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию. Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

```
perl nikto.pl -h http://localhost/dvwa/
```

Сканирование localhost

```
(artemkuzmin@artem)-[~]  
$ nikto -h http://localhost  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: localhost  
+ Target Port: 80  
+ Start Time: 2025-03-16 13:41:57 (GMT3)  
  
+ Server: Apache/2.4.63 (Debian)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 63141f9af8551, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561  
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
```

Рис. 1: Тестирование localhost

Сканирование localhost/dvwa/

```
(artemkuzmin@artem)-[~]  
$ nikto -h http://localhost/dvwa/  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: localhost  
+ Target Port: 80  
+ Start Time: 2025-03-16 13:43:37 (GMT3)  
  
+ Server: Apache/2.4.63 (Debian)  
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .  
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
```

Рис. 1: Тестирование localhost/dvwa/

Выводы

В результате выполнения работы я повысил свои навыки использования приложений с целью информационной безопасности. Также познакомился с новым софтом под названием Nikto. Мощные инструменты задействованы в этом приложении.